IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, v. KYLE SODERHOLM, Defendant.	)	4:11CR3050 MEMORANDUM AND ORDER ON THE DEFENDANT'S OBJECTIONS TO THE MAGISTRATE JUDGE'S FINDINGS, RECOMMENDATION AND ORDER

Defendant Kyle Soderholm moved to suppress evidence that was obtained by law enforcement officers during a search of the defendant's home on January 13, 2011. (ECF No. 15.) In accordance with 28 U.S.C. § 636(b)(1)(B)-(C) and Federal Rule of Criminal Procedure 59(b)(1), United States Magistrate Judge Cheryl R. Zwart has recommended that I deny the defendant's motion. (See ECF No. 24). Now before me is the defendant's "Statement of Objection to Recommendations by Magistrate Judge." (ECF No. 27.) In the course of my de novo review of those portions of the magistrate judge's findings and recommendation that the defendant challenges, see 28 U.S.C. 636(b)(1); Fed. R. Crim. P. 59(b)(3), I have studied the magistrate judge's Findings, Recommendation and Order, (ECF No. 24), the motion, objection, and briefs submitted by the parties, (ECF Nos. 15, 16, 27, 28, 32), and the exhibits submitted by the defendant, (see ECF No. 20). After reviewing these materials, I find that the magistrate judge's recommendation should be adopted. The defendant's objection will be overruled, and his motion to suppress will be denied.

I. BACKGROUND

The defendant states that he "objects to all findings made by" the magistrate judge. (Def.'s Objection at 2, ECF No. 27.) In Part II.A below, I shall address the question of whether the defendant's general objection is sufficient to trigger a de novo review of the magistrate judge's findings and recommendation. For present purposes, I note that the defendant has not suggested that any of the magistrate judge's factual findings are erroneous–though he does suggest that some of her

conclusions are not supported by the available facts. (See, e.g., Def.'s Br. in Supp. of Objections at 6-7, ECF No. 28 (arguing that there is no evidence showing that the defendant voluntarily consented to provide investigators with his password).) The magistrate judge conducted no hearing, but instead relied upon the facts set forth in the affidavit of Special Agent Jeffrey D. Tarpinian, which was attached to his application for a warrant to search the defendant's home. (See Findings, Recommendation, & Order at 2-5, ECF No. 24 (citing Tarpinian Aff., Def.'s Ex. 1, Attach. C, ECF No. 20).)[1] I shall adopt the magistrate judge's factual findings; a brief summary of the relevant background follows.

Special Agent (SA) Tarpinian states that he has twenty two years of experience with the Federal Bureau of Investigation, and at the time of the drafting of his affidavit, he was assigned to the Cyber Crime Task Force (CCTF) of the FBI's Omaha Division. (Tarpinian Aff. ¶¶ 1-2.) He has experience investigating child pornography crimes, and he has received relevant training from the FBI and from the National Center for Missing and Exploited Children. (Id. ¶ 2.)

SA Tarpinian states that on September 17, 2010, SA Barry W. Couch launched a P2P file sharing program on his computer at the Rochester, New York, FBI office. (Id. ¶ 29(a).) P2P (or "peer-to-peer") file sharing refers to "a method of communication available to Internet users through the use of special software." (Id. ¶ 6(j).) SA Tarpinian explains,

> Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer . . . and conducting searches for files that are currently being shared on another user's computer.

(Id.) He adds,

---

[1] I note in passing that the defendant appears to have submitted an incomplete copy of Special Agent Tarpinian's affidavit; the affidavit ends mid-sentence, and it lacks both a signature and date. (See generally Tarpinian Aff., Def.'s Ex. 1, Attach. C, ECF No. 20.)

I also note that it is appropriate to rely upon reliable hearsay evidence when analyzing a motion to suppress. See, e.g., United States v. Matlock, 415 U.S. 164, 172-75 (1974); Fed. R. Evid. 104(a); Fed. R. Evid. 1101(d)(1).

> The latest evolution of P2P software is a program that allows a user to set up his own private P2P network of contacts. File-sharing through this new and publically available P2P file-sharing program is limited only to other users who have been added to a private lists of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

(Id. ¶ 15.)

After SA Couch launched his P2P file sharing program, he "queried his network of friends and observed that an individual using the username 'Suckboy69' was logged onto the network." (Id. ¶ 29(a).) Because Suckboy69 provided his password to SA Crouch sometime previously, Crouch was able "to view and download files from Suckboy[69's] computer that Suckboy69 selected to share with other users." (Id. (quotation marks omitted).) SA Couch found "numerous image[s] and video files depicting child pornography" in Suckboy69's shared folders, and he downloaded 49 of these files between 2:09 am and 2:31 am Eastern Time. (Id. ¶ 29(b).) During this download, SA Couch was able to identify the IP address assigned to Suckboy69's computer. (Id.)[2] SA Couch determined that the IP address was registered to Charter Communications, and "an administrative subpoena sent to Charter Communications on September 17, 2010[,] for the date and time the files were downloaded revealed that . . . the IP address was assigned to the account registered to Kyle Soderholm, 916 11th Avenue, Holdrege, Nebraska." (Id. ¶ 29(c).)

On September 24, 2010, SA Tarpinian reviewed the files obtained by SA Couch and determined that 35 images and one video depicted child pornography. (Id. ¶ 29(d)-(e).) On December 3, 2010, SA Tarpinian discussed the investigation with Investigators Scott Haugaard and Nathan Malicky of the Nebraska State Patrol. (Id. ¶ 29(f).) Investigators Haugaard and Malicky viewed three of the files selected by SA Tarpinian and "noted" that they depicted child pornography. (Id.) After obtaining more information about the defendant, (id. ¶¶ 29(g)-(i)), SA Tarpinian completed an application for a warrant to search the defendant's home, (see id. ¶ 30). On January

[2] SA Tarpinian states that an IP address, or Internet Protocol address, is "a unique number used by a computer to access the Internet." (Tarpinian Aff. ¶ 6(h).)

11, 2011, Magistrate Judge Zwart signed both the application and the warrant. (See Warrant Application, Def.'s Ex. 1, ECF No. 20; Warrant, Def.'s Ex. 2, ECF No. 20.) The warrant was executed on January 13, 2011, and a number of items–including computers, CDs, zip drives, and VHS tapes–were seized from the defendant's residence. (See Warrant at 2, Def.'s Ex. 2, ECF No. 20; Receipt for Seized Property, Def.'s Ex. 4, ECF No. 20.)

A two-count indictment filed on May 20, 2011, charged the defendant with knowingly receiving and distributing child pornography in violation of 18 U.S.C. § 2252A(a)(2) (Count I) and knowingly possessing visual depictions of minors engaging in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B) (Count II).[3] (See generally Indictment, ECF No. 1.) On August 1, 2011, the defendant, through counsel, filed a "Motion to Suppress Evidence Obtained by the Search Warrant." (ECF No. 15.) In this motion, the defendant argued that the search of his "home and property" violated the Fourth Amendment. (See id. at 1.) More specifically, he argued that: 1) the initial "search" of the defendant's computer "by a person posing as a 'friend' on the internet" violated the Fourth Amendment; 2) the affidavit submitted in support of the search warrant application contained stale, unreliable information, and therefore did not support a finding of probable cause; and 3) the seizure and search of the defendant's computer violated the Fourth Amendment. (See id. at 2-3.) In a brief submitted in support of his motion, the defendant also argued (without elaboration) that "the information obtained by [SA] Couch violated the Electronic Communications Privacy Act of 1986 and should be suppressed." (Def.'s Br. at 2, ECF No. 16. See also id. at 19.)

On September 26, 2011, Magistrate Judge Zwart found that no hearing of the defendant's motion was necessary, and she recommended that the defendant's motion to suppress be denied. (Findings, Recommendation, & Order, ECF No. 24.) She rejected the defendant's argument that SA Couch's use of the P2P network to browse the defendant's shared computer files violated the Fourth Amendment, noting that there was no indication that SA Couch entrapped the defendant or coerced him to grant a friend request. (Id. at 6-7.) She also rejected the defendant's argument that SA

[3] The indictment also includes a "Forfeiture Allegation" stating that upon conviction, the defendant shall forfeit to the United States certain property connected with the charged offenses. (See Indictment at 2, ECF No. 1.)

Tarpinian's affidavit was insufficient, adding that "even if probable cause was lacking, the defendant has made no showing that the affiant officer intentionally or recklessly misstated or omitted material facts in his warrant application, that the [magistrate] judge completely abandoned her judicial role when issuing the warrant, or that a reasonable officer would not have relied on the warrant as authority to perform the search." (Id. at 10-11 (citing Franks v. Delaware, 438 U.S. 154 (1978); United States v. Hessman, 369 F.3d 1016, 1019 (8th Cir. 2004)).) Furthermore, she determined that "[t]he evidence found in the defendant's residence . . . is admissible under the good faith exception set forth in U.S. v. Leon, 468 U.S. 897 (1984)." (Id. at 11.)[4]

On October 6, 2011, the defendant filed a statement of objections to the magistrate judge's Findings, Recommendation, and Order. (ECF No. 27.) In the opening paragraph of this document, the defendant states that he "objects to several portions of the Findings, Recommendation, and Order issued by" the magistrate judge. (Id. at 1.) He states on page two that he "objects to all findings made by" the magistrate judge, adding that the brief accompanying his objection "outlines the legal arguments supporting the objections." (Id. at 2 (emphasis added).) In his brief, however, the defendant argues only that SA Crouch's initial search of the defendant's computer violated the defendant's Fourth Amendment rights because the search was conducted without the defendant's consent. (See generally Def.'s Br. in Supp. of Objections, ECF No. 28.)

[4] Although the magistrate judge did not address specifically the defendant's argument that SA Couch obtained information from the defendant's computer in violation of the Electronic Communications Privacy Act of 1986, she did address the investigators' use of an administrative subpoena to link Suckboy69's IP address to the defendant. (See Findings, Recommendation & Order at 9, ECF No. 24.) See also, e.g., 18 U.S.C. § 2703(c)(2)(E) (allowing government entities to use administrative subpoenas to obtain "any temporarily assigned network address" from "[a] provider of electronic communication service or remote computing service"). Although the defendant has not objected to this aspect of the magistrate judge's recommendation, I have made a careful review, and I find that there is no indication of any violation of the Electronic Communications Privacy Act in this case.

II. ANALYSIS

A. The Sufficiency of the Defendant's Statement of Objection

In response to the defendant's objection, the government argues first that the defendant's "blanket" objection "is inadequate for review by this Court and should be rejected." (Pl.'s Br. at 1, ECF No. 32.) In support of its argument, the government cites Nebraska Criminal Rule 59.2, which states that a party's statement of objections "must specify (1) the parts of the . . . findings and recommendations to which the party objects and (2) the legal basis of the objections." NECrimR 59.2(a). The rule continues, "A party's failure to state a legal argument supporting objections to an order may be considered an abandonment of the party's objections." Id.

As noted above, the defendant's statement of objections declares that "[t]he defendant objects to all findings made by [Magistrate Judge] Zwart in the Findings, Recommendation[], and Order." (Def.'s Statement of Objections at 2, ECF No. 27.) The defendant has not specified a legal basis for such a broad objection, however. Indeed, the defendant's statement of objections does not specify a legal basis for any objection, but instead refers me to "the legal arguments" outlined in the defendant's supporting brief. (Id.) The defendant's supporting brief, in turn, includes only one general legal argument (i.e., that SA Couch violated the Fourth Amendment by using a P2P file sharing network to view and download files located on the defendant's computer). (See generally Br. in Supp. of Objections, ECF No. 28.)

I find that the defendant's failure to specify the legal basis for his "blanket" objection violates Nebraska Criminal Rule 59.2. Furthermore, because the defendant's legal arguments relate only to the magistrate judge's finding that SA Couch acted lawfully, and because the defendant has not made a specific objection to any other part of the magistrate judge's findings and recommendation, I find that the defendant has abandoned his objections to all of the magistrate judge's other findings. In other words, all of the defendant's objections are deemed abandoned except for his objection to the finding that SA Couch did not violate the Fourth Amendment.

The government argues that I should deem all of the defendant's objections to be abandoned–including his objection to the magistrate judge's finding that SA Couch acted lawfully. (Pl.'s Br. at 5-6, ECF No. 32.) In support of this argument, the government notes that in his "initial brief" to the magistrate judge, the defendant argued that he could not have consented voluntarily to

SA Couch's search of his computer "because the defendant did not know that Special Agent Couch was acting in an undercover capacity." (Id. at 5.) Now, however, the defendant "focuses on cases of consent outside of the context of an undercover investigation." (Id. at 6.) In essence, the government argues that the defendant should not be allowed to create a "moving target," and it asks me to reject out-of-hand the defendant's new, "totally different" arguments. (Id. at 5-6.)

It is true that insofar as the issue of consent is concerned, the arguments raised by the defendant in the brief supporting his motion to suppress, (Def.'s Br. at 16-19, ECF No. 16), are not the same as the arguments that he raised in the brief supporting his statement of objections, (Def.'s Br. in Supp. of Objections at 5-10, ECF No. 28). In his initial brief, the defendant noted that "the burden is upon the government to [show] that consent for a search is voluntary," and he argued that the government cannot meet its burden in this case because "the defendant didn't know the person seeking access to the files on his computer was associated with law enforcement." (Def.'s Br. at 18-19, ECF No. 16.) In support of his statement of objections, however, the defendant argues that "there . . . has been no evidence to show that the consent obtained [from] the Defendant was voluntary," and "the Court is simply inferring that S.A. Couch made a request to search and seize the items found on the computer AND that the person known as Suckboy69 consented to the search." (Def.'s Br. in Supp. of Objections at 6-7, ECF No. 28 (quotation marks omitted).) He also argues for the first time that there is no evidence that Suckboy69 had authority to consent to the search of the defendant's computer, and there is no evidence that SA Couch acted within the scope of the consent given by Suckboy69. (See id. at 8-10.) I agree with the government that these new arguments were not properly presented to the magistrate judge for review.

The Eighth Circuit has held that "even when a magistrate judge is hearing a matter pursuant to his or her limited authority to make a 'recommended disposition,' 'a claimant must present all his claims squarely to the magistrate judge, that is, the first adversarial forum, to preserve them for review.'" Madol v. Dan Nelson Automotive Group, 372 F.3d 997, 1000 (8th Cir. 2004) (quoting Roberts v. Apfel, 222 F.3d 466, 470 (8th Cir. 2000). See also Roberts, 222 F.3d at 470 ("[The] purpose of referring cases to a magistrate for recommended disposition would be contravened if parties were allowed to present only selected issues to the magistrate, reserving their full panoply of contentions for the trial court." (Quoting Reciprocal Exchange v. Noland, 542 F.2d 462, 464 (8th

Cir. 1976)).) Other courts have found, however, that because 28 U.S.C. § 636(b)(1) allows the district court to "receive further evidence" after a party objects to the magistrate judge's recommendation, district courts may consider new arguments raised for the first time in an objection. E.g., Brown v. Roe, 279 F.3d 742, 744-46 (9th Cir. 2002) (citing, inter alia, Freeman v. County of Bexar, 142 F.3d 848, 850-53 (5th Cir. 2002); Paterson-Leitch Co., Inc. v. Massachusetts Municipal Wholesale Electric Co., 840 F.2d 985, 990 (1st Cir. 1988)). The Fourth Circuit has gone further, holding that "as part of its obligation to determine de novo any issue to which proper objection is made, a district court is required to consider all arguments directed to that issue, regardless of whether they were raised before the magistrate [judge]." United States v. George, 971 F.2d 1113, 1118 (4th Cir. 1992). See also id. at 1118 n.6 (noting that the district court's obligation to hear all arguments is reinforced when motions to suppress are concerned because such motions are "not one of the pretrial matters that may be reviewed by the district court merely for clear error or plain error").

Given the law in this circuit, the government's argument that I should not consider the defendant's new arguments is well-taken–though it should be noted that the government cites no cases that apply the Eighth Circuit's rule to new arguments offered in support of a motion to suppress. I shall bypass this issue, however, because I find that I can readily dispose of the defendant's new arguments on their merits.

B. Whether the Officer Violated the Fourth Amendment When He Accessed the Defendant's Shared Files Folder

The defendant objects to the magistrate judge's finding that SA Couch did not violate the Fourth Amendment when he used P2P software to view the shared files on the defendant's computer. He argues that there is no evidence that the defendant voluntarily provided his password to SA Couch; that there is no evidence indicating that Suckboy69 had authority to give consent to search the defendant's computer; and that there is no evidence that SA Couch's search was within the scope of the consent given by Suckboy69. (Def.'s Br. in Supp. of Objections at 5-10, ECF No. 28.)

In opposition to the defendant's objections, the government argues first that the Fourth Amendment does not provide any protection to the defendant because he did not have a legitimate expectation of privacy in his shared files. (Pl.'s Br. at 8-12, ECF No. 32.) It is well-established that,

in order to claim the protection of the Fourth Amendment, a person must demonstrate that he "has a legitimate expectation of privacy in the invaded place" or the items seized. Minnesota v. Carter, 525 U.S. 83, 88 (1998) (quoting Rakas v. Illinois, 439 U.S. 128, 143 (1978)). See also United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009) ("Whether a defendant has a constitutionally protected expectation of privacy involves a two-part inquiry–the defendant must show that (1) he has a reasonable expectation of privacy in the areas searched or the items seized, and (2) society is prepared to accept the expectation of privacy as objectively reasonable." (Citation omitted)). Moreover, the Eighth Circuit has held that although an individual generally "has an objectively reasonable expectation of privacy in his personal computer," this expectation cannot "survive [an individual's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." Stults, 575 F.3d at 843 (quoting United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008)).

In the instant case, the defendant used a new type of file sharing software that did not "open[] his computer to anyone else with the same freely available program." Stults, 575 F.3d at 843. Instead, the defendant's "closed" P2P program granted access only to computer users who had been designated as "friends" by the defendant. Thus, the facts of instant case may be distinguishable from those of Stults. Nevertheless, the government argues that the court's reasoning in Stults "is equally persuasive in this case." (Pl.'s Br. at 11, ECF No. 32 (citing United States v. Sawyer, 786 F. Supp. 2d 1352, 1355-56 (N.D. Ohio 2011) ("Nonetheless, despite the program affording some greater degree of privacy, the rationale of the decisions analyzing open file sharing programs is still persuasive here and the Court finds that Sawyer did not have an objectively reasonable expectation of privacy in the files that were shared . . . ."); United States v. Ladeau, Crim. No. 09-40021-FDS, 2010 WL 1427523, at *4-5 (D. Mass. April 7, 2010) ("No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access. . . . Once Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable. Because the files he claims were private were made available to anyone on the network, his expectation of privacy in those files was also objectively unreasonable.")).)

After careful consideration, I agree with the government that the defendant did not have an objectively reasonable expectation of privacy in the files stored on his computer once he designated those files for sharing with the "friends" on his private network. The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979). The fact that the defendant's files were restricted to designated "friends" does not alter the fact that the files were no longer kept private, and the defendant bore the risk that the contraband material that he shared with his "friends" would find its way into the possession of law enforcement officers. See Sawyer, 786 F. Supp. 2d 1355-56; Ladeau, 2010 WL 1427523, at *5. Because the defendant had no legitimate expectation of privacy in the files that he released to his "friends," the actions of SA Couch–who was a designated "friend"–did not implicate the Fourth Amendment.

Furthermore, even if I were to assume that the defendant had a legitimate expectation of privacy in his shared files, I agree with the magistrate judge's conclusion that SA Couch's actions did not violate the Fourth Amendment. By designating SA Couch as a "friend" on his closed P2P network, the defendant voluntarily consented to SA Couch's viewing and downloading the files that were located on the defendant's shared folder. See Sawyer, 786 F. Supp. 2d 1356-57. The record indicates that SA Couch did not exceed the scope of the defendant's consent: he browsed the files appearing in the folders that the defendant designated for sharing, and there he located files that he believed depicted child pornography. Finally, I must reject the defendant's argument that Suckboy69 lacked authority to consent to SA Couch's activities. "[A] search is lawful 'where officers reasonably rely on the consent of a third party who demonstrates apparent authority to authorize the search.'" United States v. Munoz, 590 F.3d 916, 922 (8th Cir. 2010) (quoting United States v. Nichols, 574 F.3d 633, 636 (8th Cir. 2009)). "Apparent authority is present when the facts available to the officer at the moment . . . warrant a man of reasonable caution in the belief that the consenting party had authority over the thing searched." Id. (quoting Nichols, 574 F.3d at 636 (quotation marks omitted). The record indicates that the person using the name Suckboy69 granted SA Couch's "friend" request and designated the files that would be available to "friends" in his shared folder. This is sufficient to warrant a man of reasonable caution in the belief that Suckboy69 had authority

to give SA Couch access to the shared files that were later traced to the defendant's computer in Holdrege, Nebraska.

IT IS ORDERED that:

1. the defendant's objections to the magistrate judge's findings, recommendation and order, ECF No. 27, are overruled;

2. the magistrate judge's recommendation, ECF No. 24, is adopted; and

3. the defendant's motion to suppress, ECF No. 15, is denied.

Dated November 9, 2011.

BY THE COURT

s/ Warren K. Urbom
United States Senior District Judge